NWU®

ITRI 615

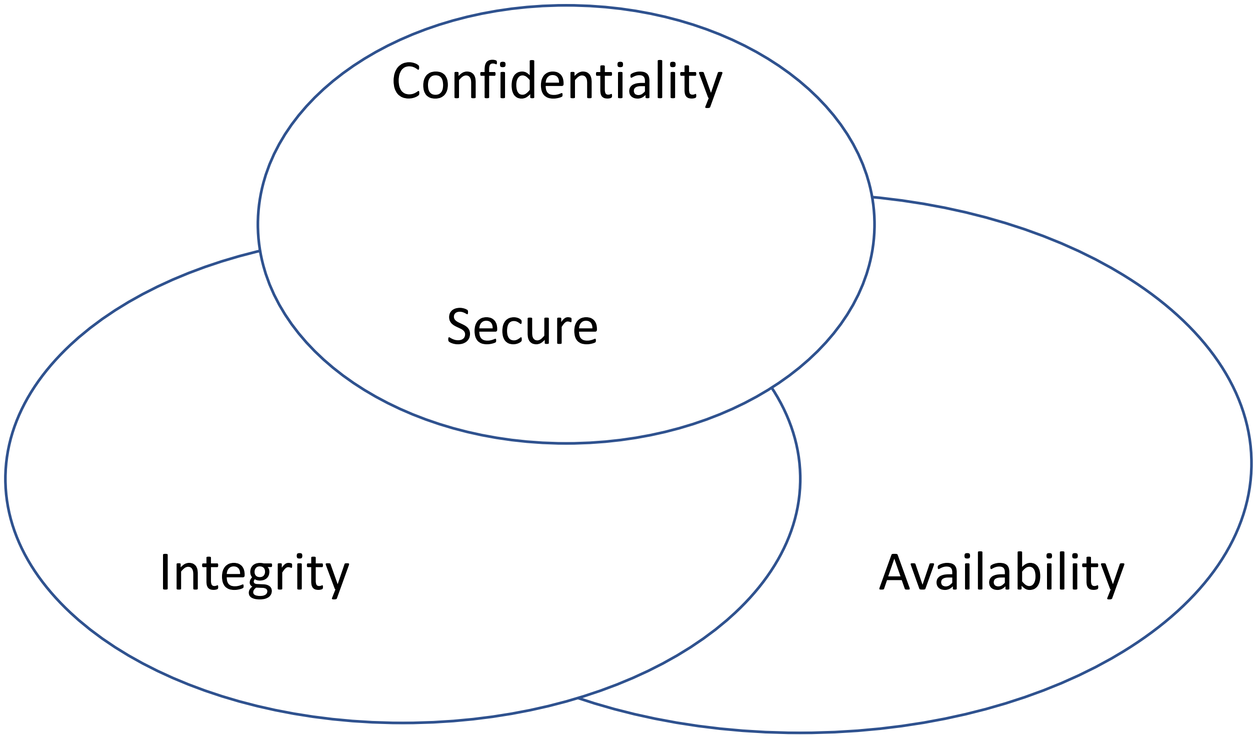
Pfleeger Chapter 1

Whitman & Mattord Chapter 1 & 2

Is there a security problem in computing?

- When do we consider something to be secure? Gold vs. data?
- For the duration of the course, a computing system will refer to the collection of hardware, software, storage media, data and people that an organization uses to perform computing tasks.
- Any system is most vulnerable at its weakest point. This leads to the principle of easiest penetration. It states that any computing system is only as strong as its weakest point.
- The four main types of threats include interception, interruption, modification and fabrication.

Objectives of computer security



Confidentiality

- Ensures that computer-related assets are accessed only by authorized parties.

- Access does not only refer to reading, but also viewing, printing, or even just knowing that a particular asset exists.

- Synonyms include secrecy and privacy.

Integrity

- Means that assets can be modified only by authorized parties or only in authorized ways.

- Modification refers to writing, changing, changing status, deleting and creating.

- It also includes error detection and correction, whereby errors, whether intentional or by accident, are identified and corrected.

Availability

- Means that assets are accessible to authorized parties at appropriate times. I.e. If a system or person has legitimate access, that access should not be prevented.

- A data item, service or system is available if

1. There is a timely response to our request.
2. Resources are allocated fairly.
3. The service or system involved follows a philosophy of fault tolerance.
4. The service or system can be used easily.
5. Concurrency is controlled.

Threats

- A threat to a computing system is a set of circumstances that has the potential to cause loss or harm.

- A threat is blocked by control of a vulnerability (weakness).

- A threat can refer to either the hardware component, the software component, the data component, or to a combination of the components.

- Threats are either human-initiated, computer-initiated, or nature-initiated.

Threats *cont.*

- The four main types of threats include:

1. Interception, where an unauthorized party has gained access to an asset.

2. Interruption, where an asset of the system has become lost, unavailable, or unusable.

3. Modification, where an unauthorized party not only accesses but tampers with an asset.

4. Fabrication, where an unauthorized party creates counterfeit objects on the computing system.

Computer criminals

- Amateurs. Ordinary computer professionals who discover they have access to something valuable.

- Crackers or malicious hackers. People that attempt to access computing facilities for which they have not been authorized.

- Career criminals. People that understand the targets of computer crime, and typically trade in companies' or individuals' secrets.

- Terrorists. People that use computers for:

1. Targets of attack.
2. Propaganda vehicles.
3. Methods of attack.

Harm

- Harm occurs when a threat is realized against a vulnerability.

- We can seek to:

1. Prevent it.

2. Deter it.

3. Deflect it.

4. Detect it.

5. Recover from its effects.

Encryption as control

- Encryption is the formal name for the scrambling process.

- Normal data, called cleartext, is taken and scrambled so that they are unintelligible to the outside observer. This takes place according to some encryption algorithm. Decryption takes place through an accompanying decryption algorithm back to its original state.

- Encryption does however not solve all computer security problems, and other tools should complement its use.

- It can be argued that weak encryption is worse that no encryption at all, as it gives users a false sense of security.

Software controls

- Programs are typically the second facet of computer security, after encryption, and includes:

1. Internal program controls. Parts that enforce security restrictions.
2. Operating system and network system controls. Limitations enforced by the operating system or network.
3. Independent control programs. Application programs that protect against certain types of vulnerabilities.
4. Development controls. Quality standards for program development.

Hardware controls

- Numerous devices have been created to assist in providing computer security, and include:

1. Hardware or smart card implementations of encryption.
2. Locks or cables limiting access or deterring theft.
3. Devices to verify users' identities.
4. Firewalls.
5. Intrusion detection systems.
6. Circuit boards that control access to storage media.

Policies and procedures as control

- Sometimes policies and procedures can be relied upon between users instead of hardware and software means.

- Something as simple as frequent password changes can have tremendous effect with no cost involved.

- Training and administration are key in reinforcing the importance of security policy.

- Legal and ethical controls are an important part of computer security, but unfortunately computing is progressing much faster than law.

Physical controls

- Some of the easiest, most effective, and least expensive controls are physical controls.

- Some examples include locks on doors, guards at entry points, backups, and physical site planning to minimize the risk of natural disasters.

- Although physical controls can have a significant impact on computer security, they are often overlooked.

Effectiveness of controls

- Controls are of no effect if they are not used properly. Several aspects that can enhance the effectiveness of controls include:

1. Awareness of problem. People using security controls will be more willing to use it if they are convinced that a problem exists.
2. Likelihood of use. No control is effective unless it is used. However, no control should seriously affect the task being protected.
3. Overlapping controls. Several different controls may apply to address a single vulnerability.
4. Periodic review. Few controls are permanently effective, and judging their effectiveness is therefore an ongoing process.

Questions

- Any Questions?